Fermat Quotient と Anomalous 楕円曲線の離散対数の多項式時間解法アルゴリズムについて(代数的整数論とその周辺)

AUTHOR(S):

佐藤, 孝和; 荒木, 純道

数理解析研究所講究録
1026巻 1998年 139-150

Fermat Quotient と Anomalous 楕円曲線の離散対数の多項式時間解法アルゴリズムについて

埼玉大学理学部数学科　佐藤孝和 (Takakazu Satoh)
tsatoh@rimath.saitama-u.ac.jp

東京工業大学工学部情報工学科　荒木純道 (Kiyomichi Araki)
araki@ss.titech.ac.jp

1. はじめに

G を群、$\alpha\in G$ を位数 $h<\infty$ である元、$\beta\in\langle\alpha\rangle$ (α により生成された巡回群) とする。したがって $n\in\mathbf{Z}/h\mathbf{Z}$ で $\beta=\alpha^n$ となるものが存在するが、この n を実際に求めることを G における**離散対数問題 (discrete log problem)** を解くという。[1] 最近のこの離散対数問題の困難性に根拠をおく公開鍵暗号・デジタル署名・鍵共有法が普及しつつあり情報通信や電子マネーの安全性といった社会的ニーズと共にその理論的な研究も盛んになってきている。

素数 p に対して p 個の元から成る有限体を $\mathbf{F}_p$ とする。$\mathbf{F}_p$ 上定義された楕円曲線は $\mathbf{F}_p$ 有理点が丁度 p 個あるとき anomalous であるという。ここでは anomalous elliptic curve $\tilde{E}$ の $\mathbf{F}_p$ 有理点に関する離散対数問題を $O((\log p)^3)$ で解くアルゴリズムを与える。すなわち、与えられた α, $\beta\in\tilde{E}(\mathbf{F}_p)-\{\mathcal{O}\}$ (ここで $\mathcal{O}$ は $\tilde{E}$ の単位元) に対して $\beta=n\alpha$ となる $n\in\mathbf{F}_p$[2] を計算時間 $O((\log p)^3)$ で求める計算手順を与える。

ここでの方法のアイディアはいわば Fermat quotient の楕円曲線版を作ることである。通常の Fermat quotient は p と互いに素な整数 a に対して $L_p(a):=\frac{a^{p-1}-1}{p}\bmod p\in\mathbf{F}_p$ と定義される。(p を底とする a の Fermat quotient という。) a, b が p と互いに素な整数ならば $L_p(ab)=L_p(a)+L_p(b)$ が $\mathbf{F}_p$ において成立する。[3] もし、仮に $L_p(a)$ が $a \bmod p$ で well defined になれば $\mathbf{F}_p^\times$ の離散対数問題は簡単にとけてしまう。すなわち、$b=a^n$ から $L_p(b)=nL_p(a)$, i.e. $n=\frac{L_p(b)}{L_p(a)}$ となるのだが実際には L_p は $\mathbf{F}_p$ 上 well defined にならない。そもそも n は $\bmod(p-1)$ で決まるが、L_p の値は $\bmod p$ で決まっているので L_p を使って $\mathbf{F}_p^\times$ の離散対数を解こうとすることに無理がある。しかし、anomalous elliptic curve $\tilde{E}$ に関して $\mathbf{F}_p$-valued な Fermat quotient の類似物が構成できれば、このような位数の compatibiliy の問題は生じないので、$\tilde{E}$ の離散対数問題を解くことができるだろうと期待できる。

1991 Mathematics Subject Classification: Primary 11G07, Secondary 94A60, 11T70
Key words and phrases: discrete logarithm, anomalous elliptic curve, Fermat quotient
本研究は両著者とも電気通信普及財団研究助成 96-01068 から部分的に補助を受けた。

[1] 離散対数問題については、1980 年代ではあるが、McCurley[10] が見やすい。

[2] $\tilde{E}$ が anomalous のとき $\tilde{E}(\mathbf{F}_p)$ は位数 p の cyclic group だから $\tilde{E}(\mathbf{F}_p)=\langle\alpha\rangle$ である。

[3] $L_p(a)$ は a の対数関数の類似と見ることもできるが、伊原 [4] に従い“関数” a の対数微分の p での値と見るほうが良いと思われる。

本稿の目的はこのような方針で実際に離散対数問題を解くことである。§2 では通常の Fermat quotient に関して知られている性質をまとめ、$(\mathbf{Z}/p^r\mathbf{Z})^\times$（ただし、$p\geq 3$, $r\geq 2$）の離散対数問題にどのように応用されるかを見る。[4] §3 で離散対数問題を応用した公開鍵暗号と楕円曲線との関連を手短に review する。§4 では $\tilde{E}$ の係数を $\mathbf{Z}$ に持ち上げた曲線 E を用いて $p\geq 7$ の時に Fermat quotient の楕円曲線版 $\lambda_E\in\mathrm{Hom}(\tilde{E}(\mathbf{F}_p),\mathbf{F}_p)$ とその計算手順を構成する。$\pi\in\mathrm{Map}(E(\mathbf{Q}_p),\tilde{E}(\mathbf{F}_p))$ を reduction mod p map とし、$u\in\mathrm{Map}(\tilde{E}(\mathbf{F}_p),E(\mathbf{Q}_p))$ を π の持ち上げ、i.e. $\pi\circ u=\mathrm{id}_{\tilde{E}(\mathbf{F}_p)}$ とする。λ_E は

$$\tilde{E}(\mathbf{F}_p)\xrightarrow{u}E(\mathbf{Q}_p)\xrightarrow{p\text{倍}}\mathrm{Ker}\,\pi\xrightarrow{\text{Formal log}}p\mathbf{Z}_p\xrightarrow{\text{mod }p^2}p\mathbf{Z}_p/p^2\mathbf{Z}_p\cong\mathbf{F}_p$$

として定義される。λ_E の実際の計算手順は系 4.6 で示される。我々のアルゴリズムは $\mathbf{Z}/p^2\mathbf{Z}$ と $\mathbf{F}_p$ の四則演算のみしか使用しない。これにより計算に必要な時間を厳密に評価でき、またこのアルゴリズムに基づいたプログラムを作成するのが容易になる。さて、λ_E は位数 p の群から位数 p への準同型写像であるから零写像か同型写像である。これが零写像であった場合、$\tilde{E}$ の持ち上げ E をうまく取り直して λ_E を同型写像にすることができることを定理 4.7 で示す。これらを合わせ、$\tilde{E}(\mathbf{F}_p)$ の離散対数問題が多項式時間で解けることが分かる。

素体上の anomalous elliptic curve の離散対数問題に関する本研究が終った後で、英国 Hewlett-Packard 研究所の Dr. N. Smart[19] が同時期に独立に同じ結果を得ていることを伝えられた。さらに、この研究集会の後、1997 年 11 月 3, 4 日とカナダの Waterloo 大学で開かれた楕円曲線の離散対数問題ワークショップにおいて Semaev[16] が既に、代数幾何的方法で $\mathbf{F}_p$ 上の楕円曲線の p-torsion point の離散対数を多項式時間で解く方法を既に 1995/96 年に得ていたこと、Semaev の方針は Rueck[15] により任意の種数の曲線の divisor class group の p-torsion point に関する離散対数問題の解法に一般化されていることを知らされた。しかしながら、Smart および我々の方法は Semaev/Rueck の方法と全く異なる。二つの方法の比較に関しては Voloch[20] が詳しい。

謝辞：第一著者は、重要な示唆を与えて下さった伊原康隆氏に感謝します。

Notation

環は常に単位的可換環とする。環 R の単数群を $R^\times$ と書く。$a\in\mathbf{Q}$ に対して

$$\mathrm{ord}_p a:=\begin{cases} r & \left(a=p^r\frac{v}{u},\quad u,v\in\mathbf{Z}-p\mathbf{Z}\right),\\ \infty & (a=0),\end{cases}$$

を正規化された加法的付値とする。$\mathbf{Q}_p$ 及び $\mathbf{Z}_p$ はそれぞれ p 進数体、p 進整数環を表す。[5] ord_p は $\mathbf{Q}_p$ から $\mathbf{Z}\cup\{\infty\}$ への連続関数に拡張されるがこれも同じ ord_p で表す。

---

[4] これらは 150~100 年位前から知られていたことではあるが、計算量の議論も含めた形で explicit に述べられたことはないようである。

[5] 暗号理論の文献ではしばしば $\mathbf{Z}/n\mathbf{Z}$ のことを $\mathbf{Z}_n$ と書いているものがあるが、もちろん、$\mathbf{Z}/p\mathbf{Z}$ と p 進整数環は全く別物である。p 進数についての解説は例えば Cassels[2] あるいは Serre[17] などを参照されたい。

2. Fermat Quotient

p を素数とする。1828 年に Abel[1] は次の問題を提起した：

> Le nombre $\alpha^{\mu-1}-1$ peut il être divisible par μ^2, μ étant un numbre premier, et α un entire moindre que μ et plus grand que l'unité?

ここで Fermat の小定理により α が p で割れないなら $\alpha^{p-1}-1$ は p^1 では常に割れることに注意する。p で割れない整数 a に対して

$$L_p(a) := \frac{a^{p-1}-1}{p} \bmod p \in \mathbf{F}_p \tag{2.1}$$

とおく。$L_p(a)$ を **Fermat quotient** という。Dickson[3, p.105] によると 1850 年に G. Eisenstein は $a,\ b\in\mathbf{Z}-p\mathbf{Z},\ c\in\mathbf{Z}$ に対して

$$\begin{cases} L_p(ab) = L_p(a)+L_p(b) \\ L_p(a+pc) = L_p(a)-ca^{-1} \end{cases} \tag{2.2}$$

となることを発見した。ここで a^{-1} は $\mathbf{F}_p$ での a の逆元である。Lerch[8, (27)] は (2.2) を法が必ずしも素数ではない場合に一般化した：整数 $m\geq 2$、および m と互いに素な整数 a に対して $L_m(a):=\frac{a^{\varphi(m)}-1}{m} \bmod m\in\mathbf{Z}/m\mathbf{Z}$ とおく。すると

$$\begin{cases} L_m(ab) = L_m(a)+L_m(b) \\ L_m(a+mc) = L_m(a)+\varphi(m)ca^{-1} \end{cases} \tag{2.3}$$

が整数 c、および m と互いに素な整数 $a,\ b$ に対して成立する。その他、Fermat quotient に関しては Dickson[3, Chap. 4] が詳しい。Abel の元の問題に関しては Jacobi[6] が $a^{p-1}\equiv 1 \bmod p^2$ の解は $p\leq 37$ で $(a,p)=(3,11),\ (9,11),\ (14,29),\ (18,37)$ に限られることを示した。しかしながら、著者らの知る限り、a を一つ選んだ時、$a^{p-1}\equiv 1 \bmod p^2$ となる p が無限個存在するかは未解決である。伊原[4] はこの問題を現代的な視点から考察している。Ribenboim[14, Chap. 5.III] によると Dilcher と Pomerance は $2^{p-1}\equiv 1 \bmod p^2$ となる p は $p<4\times 10^{12}$ の範囲では $p=1093$ と $p=3511$ のみであることを確認した。

(2.1) の解釈として次のようなものが考えられる。G を何らかの意味で $\mathbf{F}_p$ 上定義された元からなる位数 n の有限群とする。$g\in G$ を一旦 $\mathbf{Z}$ に持ち上げてから $g^n \bmod p^2$ を求める。これは p 進的な意味で G の単位元に近いはずである。この二つの差がある意味で g の微分のようなものと考えられる。次節ではこのような方針で楕円曲線上の Fermat Quotient を構成する。

Fermat quotient と離散対数との関連を見るために、$p\geq 3$ かつ $r\geq 2$ の時の $(\mathbf{Z}/p^r\mathbf{Z})^\times$ の離散対数問題について考えよう。$\omega\in\mathbf{Z}$ を $\bmod p^2$ の原始根とする。この時、良く知られているように ω はすべての $r\geq 1$ に対して $\bmod p^r$ の原始根になる。ここで $\alpha\in(\mathbf{Z}/p^r\mathbf{Z})^\times$ を任意にとる。

$$\alpha \equiv \omega^n \bmod p^r \tag{2.4}$$

となる $n\in\mathbf{Z}/p^{r-1}(p-1)\mathbf{Z}$ を求めることが目標である。p で割れない整数 a に対して (2.3) より $L_{p^r}(a+p^r)=L_{p^r}(a)-p^{r-1}a^{-1}$ である。ゆえに L_{p^r} は写像 $(\mathbf{Z}/p^r\mathbf{Z})^\times\to\mathbf{Z}/p^{r-1}\mathbf{Z}$ を導く。これも同じ記号

L_{p^r} により表すことにする。(2.3) より $L_{p^r}(\alpha)\equiv nL_{p^r}(\omega) \bmod p^{r-1}$ である。ここで、定義により $\omega^{p-1} \equiv 1+pL_p(\omega) \bmod p^2$ である。ところが $\omega^{p-1}\not\equiv 1 \bmod p^2$ なのだから $L_p(\omega)\in \mathbf{F}_p^\times$ である。他方、$\omega^{(p-1)p^{r-1}} \equiv (1+pL_p(\omega))^{p^{r-1}} \bmod p^{r+1}$. $p\geq 3$ なので $\omega^{(p-1)p^{r-1}}\equiv 1+p^rL_p(\omega) \bmod p^{r+1}$ となる。(cf. Ireland and Rosen[5, Chap. 4, Sect. 1, Lemma 3 and Corollary 1]) ゆえに $L_{p^r}(\omega)\equiv L_p(\omega) \bmod p$, i.e., $L_{p^r}(\omega)\in(\mathbf{Z}/p^r\mathbf{Z})^\times$ である。従って

$$n \equiv \frac{L_{p^r}(\alpha)}{L_{p^r}(\omega)} \bmod p^{r-1} \tag{2.5}$$

を得る。他方、(2.4) を $\bmod p$ すると $\alpha\equiv\omega^n \bmod p$ となる。$\mathbf{F}_p^\times$ の離散対数アルゴリズムを何かしら適用して

$$n \equiv k \bmod p-1. \tag{2.6}$$

となる k が求まる。(2.5) と (2.6) に Chinese remainder theorem を使って n の値を得る。$T(p)$ を $\mathbf{F}_p$ の離散対数を解く時間計算量とすると、上の方法の時間計算量は $O(T(p)+(\log p^r)^2\log r)$ である。[6] これは Pohlig-Hellman アルゴリズム [13] よりも速い。

3. 離散対数と公開鍵暗号

本稿の暗号理論的背景として離散対数問題が実際の公開鍵暗号にどのように用いられるのか見てみよう。現代の情報通信では通信の対象となるもの（数値、文章、音声、画像など）はすべてデジタル情報（0 と 1 の有限列）として良い。長いものは予め決めておいた長さ N に区切って順次通信すれば良い。このような 0, 1 からなるN 個の列は 0 以上 2^N 未満の整数、あるいは（$\mathbf{F}_{2^N}/\mathbf{F}_2$ の基底を決めておいて）$\mathbf{F}_{2^N}$ の元と同一視される。実用上は 0 を除いても差し支えなく、公開鍵暗号理論の目的は「予め決められた有限体の乗法群の元を**秘密鍵**と呼ばれる情報を知らない第三者には洩れないように伝える」ことと定式化される。一般に、暗号化する前の情報を**平文**、暗号化した後の情報を**暗号文**、秘密鍵を使って暗号文から平文を得ることを**復号**、秘密鍵を使わずに平文（または秘密鍵そのもの）を得ることを**解読**という。暗号化に際しては公開鍵と呼ばれる情報を使うが、これは全員に公開されているので、誰でもが暗号化できることになる。

q を素数べき[7] とする。$\mathbf{F}_q^\times$ の離散対数の困難性に基づく公開鍵暗号の一例として ElGamal 暗号系を解説する。この暗号系では平文は $\mathbf{F}_q^\times$ の元、暗号文は $\mathbf{F}_q^\times\times\mathbf{F}_q^\times$ の元である。

事前の設定

受信者は素数べき q, $\mathbf{F}_q^\times$ の生成元 α, $c\in(\mathbf{Z}/(q-1)\mathbf{Z})^\times$ を選び、$\beta:=\alpha^c$ を計算する。そして、q, α, β を公開する。c は受信者だけが知っている秘密情報（秘密鍵）とする。

暗号化

送信者は平文x が与えられた時 $k\in(\mathbf{Z}/(q-1)\mathbf{Z})^\times$ をランダムに選ぶ。そして $(\alpha^k, x\beta^k)$ の値を計算し、その結果を暗号文とする。

---

[6] ここで、$L_{p^r}(a) \bmod p^{r-1}$ を計算するには $a^{p^r-p^{r-1}} \bmod p^{2r-1}$ が分かれば十分であることに注意する。

[7] 実用上は q は 2^N より少し大きい素数か 2^N のいずれかにする。

復号化

受信者は暗号文 (y_1, y_2) を受けとったら $y_1^{-c}y_2$ を計算し、平文を得る。

$\mathbf{F}_q^\times$ の離散対数が解ければこの暗号は簡単に解読されてしまう。[8]

群として $\mathbf{F}_q^\times$ の代わりに有限体 $\mathbf{F}_q$ 上の楕円曲線 E の $\mathbf{F}_q$ 有理点のなす群を使った場合の暗号化・復号化の手順は自明であろう。ところが、このままでは問題が生じる。(全てが 0 ではない) 0, 1 の N 個の列を $\mathbf{F}_p^\times$ (ここで p は 2^N より大きい素数) や $\mathbf{F}_{2^N}^\times$ に埋め込むのは簡単・高速であるが、楕円曲線上の点と対応させるのは自明ではない。この解決策もいろいろあるが、一例として Menezes-Vanstone による方法を挙げる。この方法では平文は $\mathbf{F}_q^\times \times \mathbf{F}_q^\times$, 暗号文は $E(\mathbf{F}_q)\times \mathbf{F}_q^\times \times \mathbf{F}_q^\times$ の元である。

事前の設定

受信者は素数べき q, 楕円曲線 $E/\mathbf{F}_q$, $E(\mathbf{F}_q)$ の位数が大きな (かつ大きな素因数を含む) 点 α を選ぶ。α の位数を h とし、$c \in (\mathbf{Z}/h\mathbf{Z})^\times$ を選び、$\beta := c\alpha$ を計算する。そして、q, E, α, h, β を公開する。c は受信者だけが知っている秘密情報とする。

暗号化

平文 $(x_1, x_2) \in \mathbf{F}_q^\times \times \mathbf{F}_q^\times$ が与えられた時 $k \in (\mathbf{Z}/h\mathbf{Z})^\times$ をランダムに選ぶ。そして $k\beta$ の affine 座標 (m_1, m_2) を求め、$(k\alpha, m_1x_1, m_2x_2)$ を計算し、その結果を暗号文とする。

復号化

受信者は暗号文 (y_0, y_1, y_2) を受けとったら cy_0 の affine 座標 (l_1, l_2) を求め、$(y_1l_1^{-1}, y_2l_2^{-1})$ を計算し、平文を得る。

ところで、なぜここまでして[9] 楕円曲線を用いるのだろうか？これは単に「楕円曲線の方がなんとなく複雑そうだから解読に手間がかかるだろう」などという理由からではない。有限体の乗法群の離散対数問題の有力な解法として index calculus method というものがあるがこれが楕円曲線には (少なくともそのままでは) 適用できないのである。これは Mordell-Weil の定理の帰結 (genus 0 と genus ≥ 1 の差) なのであるが、紙数の都合で割愛する。[10] このことから、

$$\text{楕円曲線の離散対数の難しさ} > \text{有限体の離散対数の難しさ} \tag{3.1}$$

と予想されていたのだが、Menezes-Okamoto-Vanstone[11] により E が supersingular ならば Weil-pairing を用いて $E/\mathbf{F}_q$ の離散対数を $\mathbf{F}_{q^m}^\times$ (m は E によって決まる 6 以下の自然数) の離散対数に帰着させられることが判明した。よって up to sub-exponential time で (3.1) の $>$ は $\geq$ とせねばならないのだが、不等号の向きが逆になることはないと思われていた。しかしながら、次節で示されるように $E/\mathbf{F}_p$ が anomalous ならばこの不等号の向きが真に逆転してしまう、しかも、離散対数が多項式時間で解けてしまうのである。

---

[8] 逆に、この暗号が解ければ離散対数が解けるか (c の値を求めることを経由せずに直接解読できるか) ということは「今のところ」分かってない。

[9] 実用的な見地からは上記のような工夫の他、楕円曲線上の加法をいかに高速に実行するかなど解決しなくてはいけない課題がたくさんある。

[10] 有限体上の楕円曲線を用いる暗号系は Miller[12] と Koblitz[7] により独立に発見されたが、Mordell-Weil の定理との関連に基づく考察は Miller によるものである。詳しくは Miller[12] を参照されたい。

4. Anomalous Elliptic Curve の離散対数

p を素数、

$$\tilde{E} : y^2+\tilde{a}_1xy+\tilde{a}_3y = x^3+\tilde{a}_2x^2+\tilde{a}_4x+\tilde{a}_6$$

を $\mathbf{F}_p$ 上の楕円曲線とする。Mazur[9] に従い、$^{\#}\tilde{E}(\mathbf{F}_p)=p$ のとき $\tilde{E}$ を **anomalous** という。[11] E を $\tilde{E}$ の $\mathbf{Z}$ への（係数毎の）持ち上げとする。すなわち、$a_i \bmod p=\tilde{a}_i$ となる $a_i\in\mathbf{Z}$ を選び、E を

$$E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

により定義する。$\mathbf{P}^2(\mathbf{Q}_p)$ から $\mathbf{P}^2(\mathbf{F}_p)$ への reduction $\bmod p$ map を π とする。[12] π により $E(\mathbf{Q}_p)$ の点は $\tilde{E}(\mathbf{F}_p)$ に移される。一般に楕円曲線の群演算に関する単位元を $\mathcal{O}$ と書く。$\mathbf{Z}$-algebra R に対して

$$E(R) := \{(x:y:1)\in\mathbf{P}^2(R) : y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{(0:1:0)\}$$

とおく。R が体でない場合には $E(R)$ は必ずしも群ではないことに注意する。多少乱暴ではあるが、この場合も $(0:1:0)$ を $\mathcal{O}$ と書くことにする。また、射影空間の点 $(X:Y:1)\in\mathbf{P}^2(R)$ を $(X,Y)\in\mathbf{A}^2(R)$ と同一視する。$\mathcal{E}$ を E の形式群としよう。[13] このとき同型写像 $\mathcal{L}$ が以下により定義される。

$$\mathcal{L} : \mathrm{Ker}\pi \xrightarrow{\psi} \mathcal{E}(p\mathbf{Z}_p) \xrightarrow{\log_{\mathcal{E}}} p\mathbf{Z}_p \tag{4.1}$$

ここで $\psi(x:y:z)=x/y$,[14] $\log_{\mathcal{E}}$ は $\mathcal{E}$ の形式対数

$$\log_{\mathcal{E}}(t) := t-\frac{a_1}{2}t^2+\frac{a_1^2+a_2}{3}t^3-\frac{a_1^3+2a_1a_2+a_3}{4}t^4+\frac{a_1^4+3a_1^2a_2+6a_1a_3+a_2^2+2a_4}{5}t^5-\cdots \tag{4.2}$$

である。

以下、$\tilde{E}$ を **anomalous elliptic curve** とする。次の補題はほとんど自明であるが、我々の方法のキーポイントとなる。

補題 4.1. $pE(\mathbf{Q}_p)\subset\mathrm{Ker}\pi$.

証明 . $A\in E(\mathbf{Q}_p)$ を任意とする。Silverman[18, Chap 7, proof of Prop. 2.1] にあるように π は群の準同型である。従って $\tilde{E}$ が anomalous であることを用いると $\pi(pA)=p\pi(A)=\mathcal{O}$. ■

---

[11] もともと Mazur は楕円曲線 $E/\mathbf{Q}$ と素数 p に対して E が p で good reduction を持ち、Frobenious at p の trace が $1 \bmod p$ であるときに p を E の anomalous prime と呼んだ。

[12] すなわち、$\mathbf{Z}_p$ から $\mathbf{F}_p$ への reduction $\bmod p$ map を π' とすると

$$\pi((x:y:z)) = (\pi'(p^{-m}x):\pi'(p^{-m}y):\pi'(p^{-m}z)) \qquad \text{但し} \quad m := \min(\mathrm{ord}_p x, \mathrm{ord}_p y, \mathrm{ord}_p z)$$

である。

[13] 楕円曲線に付随する形式群の定義と基本的な性質に関しては Silverman[18, Chap. 4] などを参照されたい。

[14] $\mathcal{O}$ での local parameter の取り方は Silverman[18] のそれとは符号が逆であるが、本質的な差異はない。

定理 4.2. u を $\tilde{E}(\mathbf{F}_p)$ から $E(\mathbf{Q}_p)$ への任意の持ち上げ、すなわち $\pi\circ u=\mathrm{id}_{\tilde{E}(\mathbf{F}_p)}$ を満たす写像とする。λ_E を以下の写像の合成とする。

$$\lambda_E : \tilde{E}(\mathbf{F}_p) \xrightarrow{u} E(\mathbf{Q}_p) \xrightarrow{h_p} \mathrm{Ker}\pi \xrightarrow{\mathscr{L}} p\mathbf{Z}_p \xrightarrow{\mathrm{mod}\ p^2} p\mathbf{Z}_p/p^2\mathbf{Z}_p \cong \mathbf{F}_p. \qquad (4.3)$$

ここで h_p は p 倍写像である。この時、λ_E は u の選び方に依らない群の準同型写像である。さらに、λ_E は零写像か同型写像のいずれかである。

証明． $\alpha,\ \beta\in\tilde{E}(\mathbf{F}_p)$ とし $\Delta:=u(\alpha)+u(\beta)-u(\alpha+\beta)$ とおく。π は群準同型写像で u は持ち上げなのだから $\pi(\Delta)=\mathcal{O}$, i.e. $\Delta\in\mathrm{Ker}\pi$ となる。(4.1) により $\mathscr{L}(\Delta)=pt_0$ となる $t_0\in\mathbf{Z}_p$ が存在する。従って $\mathscr{L}(h_p(\Delta))=p^2t_0\in p^2\mathbf{Z}_p$. $F:=(\mathrm{mod}\,p^2)\circ\mathscr{L}\circ h_p$ とおくと、$F(\Delta)=0$ である。F は群準同型だから $F(u(\alpha))+F(u(\beta))\ =\ F(u(\alpha+\beta))$ となり、λ_E が準同型写像であることが示された。v を別の持ち上げ $v:\tilde{E}(\mathbf{F}_p)\to E(\mathbf{Q}_p)$ とする。すると任意の $\alpha\in\tilde{E}(\mathbf{F}_p)$ に対して $\pi(u(\alpha)-v(\alpha))\ =\ \pi(u(\alpha))-\pi(v(\alpha))\ =\ \mathcal{O}$ となる。よって、$u(\alpha)-v(\alpha)\in\mathrm{Ker}\pi$ であり、上と同様な議論で $F(u(\alpha))=F(v(\alpha))$ となる。従って λ_E は u の選び方に依らない。最後に、$\tilde{E}(\mathbf{F}_p)$ は位数 p の群だから $\mathrm{Ker}\lambda_E$ は $\tilde{E}(\mathbf{F}_p)$ か $\{\mathcal{O}\}$ のどちらかでねばならない。前者なら λ_E は零写像、後者なら同型写像となる。[15] ■

注意 4.3. λ_E は u の選び方には依存しないが、E の選び方には依存する。定理 4.7 参照。

系 4.4. $\tilde{E}$ を $\mathbf{F}_p$ 上の anomalous elliptic curve とし E をその $\mathbf{Z}$ への持ち上げとする。この時以下は同値である。

(i) λ_E は零写像。

(ii) $\alpha\in\tilde{E}(\mathbf{F}_p)-\{\mathcal{O}\}$ で $\lambda_E(\alpha)=0$ となるものが存在する。

(iii) $E(\mathbf{Z}_p)-\{\mathcal{O}\}$ に属する $\dot{E}$ の p-torsion point が存在する。

証明． (i)→(ii) は自明。(ii)→(i): $\alpha\in\tilde{E}(\mathbf{F}_p)-\{\mathcal{O}\}$ が $\lambda_E(\alpha)=0$ を満たすとする。$\tilde{E}(\mathbf{F}_p)$ は位数 p の巡回群だから α はその生成元であり任意の $\beta\in\tilde{E}(\mathbf{F}_p)$ に対して $\beta=n\alpha$ となる $n\in\mathbf{N}$ がある。ゆえに $\lambda_E(\beta)=n\lambda_E(\alpha)=0$.

(ii)→(iii): $\alpha\in\tilde{E}(\mathbf{F}_p)-\{\mathcal{O}\}$ が $\lambda_E(\alpha)=0$ となっているとする。従って $\mathscr{L}(pu(\alpha))=p^2t_1$ となる $t_1\in\mathbf{Z}_p$ が存在する。$B:=\mathscr{L}^{-1}(pt_1)\in\mathrm{Ker}\pi$ とおく。$\mathscr{L}$ は同型写像だから $pB=pu(\alpha)$ である。$A:=u(\alpha)-B$ とおくと A は p-torsion point である。また、$\pi(A)=\pi(u(\alpha))-\pi(B)=\alpha\neq\mathcal{O}$ となるが、$\mathrm{Ker}\pi=E(\mathbf{Q}_p)-(E(\mathbf{Z}_p)-\{\mathcal{O}\})$ だから $A\in E(\mathbf{Z}_p)-\{\mathcal{O}\}$

(iii)→(ii): $A\in E(\mathbf{Z}_p)-\{\mathcal{O}\}$ かつ $pA=\mathcal{O}$ とする。$\alpha:=\pi(A)$ とおく。すると

$$\lambda_E(\alpha)\ =\ ((\mathrm{mod}\ p^2)\circ\mathscr{L})(pA)\ =\ \mathcal{O}.$$

他方、$A\in E(\mathbf{Z}_p)-\{\mathcal{O}\}$ だから $\alpha\neq\mathcal{O}$。■

---

[15] $\mathrm{Ker}\lambda_E=\{\mathcal{O}\}$ から直接従うのは λ_E の単射性であるが、$\tilde{E}(\mathbf{F}_p)$ も $\mathbf{F}_p$ も共に要素の個数は p だから λ_E が単射なら全射でなければならない。

以下、簡単のため $p\geq 5$ とする。この場合、一般性を失うことなく $\tilde{a}_1=\tilde{a}_2=\tilde{a}_3=0$ (in $\mathbf{F}_p$) かつ $a_1=a_2=a_3=0$ (in $\mathbf{Z}$) と仮定して良い。

定理 4.5. $p\geq 5$ を素数とする。$\alpha\in\tilde{E}(\mathbf{F}_p)-\{\mathcal{O}\}$ とする。$A:=(x_1,y_1)\in E(\mathbf{Z}_p)$ は $\pi(A)=\alpha$ を満たすとする。$nA\neq\mathcal{O}$ となる $n\in\mathbf{N}$ に対して nA の affine 座標を (x_n,y_n) とする。λ_E が零写像でなければ以下が成立する。

(i) $1\leq n<p$ なら $nA\in E(\mathbf{Z}_p)-\{\mathcal{O}\}$

(ii) $1\leq n<m<p$ かつ $n+m\neq p$ なら $x_n\not\equiv x_m \bmod p$

(iii) $y_{p-1}-y_1\in\mathbf{Z}_p^\times$, $\dfrac{x_{p-1}-x_1}{p}\in\mathbf{Z}_p^\times$, かつ $\lambda_E(\alpha)=\dfrac{x_{p-1}-x_1}{p(y_{p-1}-y_1)} \bmod p$

証明. (i) 最初に $1\leq n<p$ なら $nA\neq\mathcal{O}$ となることに注意する。[16] ゆえに $nA\in E(\mathbf{Z}_p)$ となることを証明しさえすれば良い。$n=1$ の時はこれは仮定の一部である。$n=2$ の時は

$$y_1 \not\equiv 0 \mod p \tag{4.4}$$

だから[17] E の群演算の公式より

$$x_2 = c_2^2-2x_1, \qquad y_2 = -c_2x_2-d_2,$$

ここで

$$c_2 = \frac{3x_1^2+a_4}{2y_1}, \qquad d_2 = \frac{-x_1^3+a_4x_1+2a_6}{2y_1}$$

となる。$y_1\in\mathbf{Z}_p^\times$ だから $x_2,\ y_2\in\mathbf{Z}_p$ となり、(i) は $n=2$ の時も成立する。$3\leq n<p$ に対しては n に関する帰納法を使う。$A,\ (n-1)A\in E(\mathbf{Z}_p)-\{\mathcal{O}\}$ とする。特に

$$\pi(A) = (x_1 \bmod p,\ y_1 \bmod p)$$
$$\pi((n-1)A) = (x_{n-1} \bmod p,\ y_{n-1} \bmod p)$$

となる。$x_1\equiv x_{n-1} \bmod p$ と仮定すると $\pi(A)=\pm\pi((n-1)A)$, i.e., $n\alpha=\mathcal{O}$ または $(n-2)\alpha=\mathcal{O}$ を得る。$\tilde{E}$ は anomalous だから $\alpha=\mathcal{O}$ となり、再び矛盾。ゆえに $x_1\not\equiv x_{n-1} \bmod p$ であり、当然、$x_1\neq x_{n-1}$ でねばならない。よって群演算の公式から

$$x_n = c_n^2-x_1-x_{n-1}, \qquad y_n = -c_n^3+c_n(x_1+x_{n-1})-d_n, \tag{4.5}$$

ここで

$$c_n = \frac{y_{n-1}-y_1}{x_{n-1}-x_1}, \qquad d_n = \frac{y_1x_{n-1}-y_{n-1}x_1}{x_{n-1}-x_1}. \tag{4.6}$$

$x_{n-1}\not\equiv x_1 \bmod p$ だったから $x_{n-1}-x_1\in\mathbf{Z}_p^\times$ であり $c_n,\ d_n\in\mathbf{Z}_p$. 従って $x_n,\ y_n\in\mathbf{Z}_p$.

(ii) の証明も同様である。$x_n\equiv x_m \bmod p$ と仮定すると $\pi(nA)=\pm\pi(mA)$, i.e., $(m\pm n)\alpha=\mathcal{O}$ であり、(i) と同じ方法で矛盾を生じる。

---

[16] 実際、$nA=\mathcal{O}$ ならば $n\alpha=\pi(nA)=\mathcal{O}$. $\tilde{E}$ は anomalous だから $\alpha=\mathcal{O}$ となり矛盾。

[17] もし $y_1\equiv 0 \bmod p$ なら $2\alpha = 2\pi(A) = 2(x_1 \bmod p, 0) = \mathcal{O}$ となり、$\tilde{E}$ が anomalous だから $\alpha=\mathcal{O}$ となってしまうが、これは仮定に反する。

(iii): $\lambda_E \neq 0$ だから $pA \neq \mathcal{O}$ (cf. 系 4.4)。(4.5) と (4.6) が $n=p$ に対して成立することに注意する。pA の affine 座標を (x_p, y_p) とする。すると $\pi((x_p:y_p:1))=\mathcal{O}=(0:1:0)$ だから $\mathrm{ord}_p y_p < 0$ かつ $\mathrm{ord}_p x_p > \mathrm{ord}_p y_p$ となる。(ii) より A, $(p-1)A \in E(\mathbf{Z}_p)$。$s := \mathrm{ord}_p c_p$ とおく。$s \geq 0$, i.e. $c_p \in \mathbf{Z}_p$ と仮定しよう。(4.6) 第二式を変形すると

$$d_p = y_1 - x_1 c_p \tag{4.7}$$

となるから $d_p \in \mathbf{Z}_p$ であり、$y_p \in \mathbf{Z}_p$ を得る。これは $\pi((x_p:y_p:1))=\mathcal{O}$ に矛盾する。従って $s<0$ である。すると (4.5) より

$$\mathrm{ord}_p x_p = 2s. \tag{4.8}$$

(4.7) からは

$$\begin{aligned} \mathrm{ord}_p d_p &\geq \min(\mathrm{ord}_p y_1, \mathrm{ord}_p x_1 + \mathrm{ord}_p c_p) \\ &\geq \mathrm{ord}_p c_p = s \end{aligned}$$

を得る。さらに $\mathrm{ord}_p(c_p(x_1+x_{p-1})) \geq s$ となるが、他方、$\mathrm{ord}_p c_p^3 = 3s < s$ である。ゆえに (4.5) から

$$\mathrm{ord}_p y_p = 3s. \tag{4.9}$$

よって $\mathrm{ord}_p \psi(pA) = \mathrm{ord}_p(x_p/y_p) = -s > 0$. 従って (4.2) より $\mathrm{ord}_p \mathscr{L}(pA) = -s$. 他方、仮定から $\lambda_E(A) \neq 0$. ゆえに $\mathrm{ord}_p \mathscr{L}(pA) = 1$. 以上をまとめて $s=-1$, $\dfrac{x_p}{py_p} \in \mathbf{Z}_p^\times$, そして $\lambda_E(A) = \dfrac{x_p}{py_p} \bmod p$ であることが分かった。$\tilde{E}$ が anomalous だから $\pi((p-1)A) = -\pi(A)$ ゆえ $y_{p-1} \equiv -y_1 \bmod p$. 従って $y_{p-1} - y_1 \equiv -2y_1 \not\equiv 0 \bmod p$. 結局 $y_{p-1} - y_1 \in \mathbf{Z}_p^\times$ である。$\mathrm{ord}_p c_p = -1$ であったから

$$\frac{x_{p-1}-x_1}{p} \in \mathbf{Z}_p^\times. \tag{4.10}$$

ここで $\hat{x} := p^2 x_p$, $\hat{y} := p^3 y_p$ とおく。(4.8), (4.9) および $s=-1$ を用いると $\hat{x}$, $\hat{y} \in \mathbf{Z}_p^\times$ を得る。よって $\lambda_E(A) = \dfrac{\hat{x}}{\hat{y}} \bmod p = \dfrac{\hat{x} \bmod p}{\hat{y} \bmod p}$. $s=-1$ だから $pc_p \in \mathbf{Z}_p^\times$ である。従って

$$\begin{aligned} \hat{x} \bmod p &= (p^2 c_p^2 - p^2(x_1 + x_{p-1})) \bmod p \\ &= (pc_p)^2 \bmod p \end{aligned}$$

かつ

$$\begin{aligned} \hat{y} \bmod p &= -p^3 c_p^3 + (pc_p)p^2(x_1 + x_{p-1}) - p^3 d_p \bmod p \\ &= -(pc_p)^3 \bmod p. \end{aligned}$$

これから

$$\lambda_E(\alpha) = \frac{(pc_p)^2 \bmod p}{-(pc_p)^3 \bmod p} = \left(-\frac{1}{p}\frac{x_{p-1}-x_1}{y_{p-1}-y_1}\right) \bmod p. \tag{4.11}$$

以上で定理は完全に証明された。■

系 4.6. $p \geq 5$ を素数、

$$\tilde{E} : y^2 = x^3 + \tilde{a}_4 x + \tilde{a}_6$$

を $\mathbf{F}_p$ 上の anomalous elliptic curve とする。$a_4 \bmod p = \tilde{a}_4$, $a_6 \bmod p = \tilde{a}_6$ を満たす整数 a_4, a_6 を選ぶ。$\mathbf{Z}$ 上の楕円曲線 E を

$$E : y^2 = x^3 + a_4 x + a_6$$

により定義する。λ_E を (4.3) により定義される準同型写像とする。この時、$\alpha := (s, t) \in \tilde{E}(\mathbf{F}_p) - \{\mathcal{O}\}$ に対して以下の手順は $\lambda_E(\alpha)$ を時間計算量 $O((\log p)^3)$ で計算する。

(i) $X_1 \bmod p = s$ and $Y_1 \bmod p = t$ となる $A := (X_1, Y_1) \in E(\mathbf{Z}/p^2\mathbf{Z})$ を見つける。

(ii) $(X_{p-1}, Y_{p-1}) := (p-1)A \in E(\mathbf{Z}/p^2\mathbf{Z})$ を楕円曲線の加法を用いて求める。

(iii) もし $X_{p-1} \neq X_1$ (in $\mathbf{Z}/p^2\mathbf{Z}$) なら

$$\lambda_E(\alpha) = \left(\frac{X_{p-1} - X_1}{p} \bmod p\right)((Y_{p-1} - Y_1) \bmod p)^{-1},$$

そうでなければ $\lambda_E(\alpha) = 0$ である。

証明． $\lambda_E(\alpha)$ を求めるには、定理 4.5 の記号の基で $y_{p-1} - y_1 \bmod p$ と $\frac{1}{p}(x_{p-1} - x_1) \bmod p$ が分かれば十分であることに注意する。(i) のためには X_1, $y \in \mathbf{Z}/p^2\mathbf{Z}$ を $X_1 \bmod p = s$ かつ $y \bmod p = t$ となるようにとり、以下の式を満たす w を求める。

$$(y + pw)^2 = X_1^3 + a_4 X_1 + a_6 \bmod p^2,$$

$$\text{i.e.} \qquad 2tw = \frac{X_1^3 + a_4 X_1 + a_6 - y^2}{p} \bmod p.$$

(この右辺は well defined であることに注意。) (4.4) によりこのような $w \in \mathbf{F}_p$ は一意的に定まる。そこで $Y_1 := y + pw$ とおけば良い。[18] すると定理 4.5(ii) から $(p-1)A \bmod p^2$ を求めるには $\mathbf{Z}/p^2\mathbf{Z}$ の四則しか使わないことが分かる。(4.10) より $\lambda_E \neq 0$ なら $X_{p-1} \neq X_1$ である。この場合、(iii) は定理 4.5(iii) から従う。そうでなければ λ_E は零写像でなければならず、$\lambda_E(\alpha) = 0$ である。

(i) と (iii) の計算に含まれる $\mathbf{Z}/p^2\mathbf{Z}$ の四則の数は p は $\tilde{E}$ と無関係である。(ii) のためには楕円曲線上の足し算を高々 $2\log_2 p$ 回行なえば良い。合計して $\lambda_E(\alpha)$ の時間計算量は $O((\log p)^3)$ である。
■

定理 4.7. E と $\tilde{E}$ を系 4.6 のとおりとし、$A := (x_1, y_1) \in E(\mathbf{Z}_p) - \{\mathcal{O}\}$ とする。

$$3x_1^2 \not\equiv -a_4 \bmod p \tag{4.12}$$

と仮定する。$a'_4 := a_4 + p$, $a'_6 := a_6 - px_1$ とおき、楕円曲線 E' を

$$E' : y^2 = x^3 + a'_4 x + a'_6$$

により定義する。[19] $(p-1)A$ を E および E' 上の加法で計算した結果（の affine 座標）をそれぞれ (x_{p-1}, y_{p-1}), (x'_{p-1}, y'_{p-1}) とする。この時、以下が成立する。

---

[18] これは Serre[17, Chap 2, §2.2] を楕円曲線の場合に具体的に書き下したものに過ぎない。

[19] $A \in E(\mathbf{Z}_p) \cap E'(\mathbf{Z}_p)$ に注意。

(i) $x_{p-1} \not\equiv x'_{p-1} \bmod p^2$ と $y_{p-1} \not\equiv y'_{p-1} \bmod p^2$ のうち少なくとも片方は成立する。
(ii) λ_E と $\lambda_{E'}$ のうち少なくとも片方は零写像ではない。

証明． (i): $x_{p-1} \equiv x'_{p-1} \bmod p^2$ かつ $y_{p-1} \equiv y'_{p-1} \bmod p^2$ と仮定する。$1 \le n \le p-1$ に対して E 上で nA を計算した結果を (x_n, y_n) で表し、E' 上で nA を計算した結果を (x'_n, y'_n) で表す。$n \ge 3$ の時、$(n-1)A = nA + (-A)$ を E 上の楕円曲線の加法公式を用いて具体的に書くと

$$x_{n-1} = \hat{c}_n^2 - x_1 - x_n, \qquad y_{n-1} = -\hat{c}_n^3 + \hat{c}_n(x_1 + x_n) - \hat{d}_n$$

ここで

$$\hat{c}_n = \frac{y_n + y_1}{x_n - x_1}, \qquad \hat{d}_n = -\frac{y_1 x_n + y_n x_1}{x_n - x_1}$$

となる。同様な式は (x'_{n-1}, y'_{n-1}) に対しても成立している。ところが、これらの式は楕円曲線を定義している Weierstrass 方程式の係数を陽に含んでいない。定理 4.5(ii) より $x_n \equiv x'_n \bmod p^2$ かつ $y_n \equiv y'_n \bmod p^2$ ならば $x_{n-1} \equiv x'_{n-1} \bmod p^2$ かつ $y_{n-1} \equiv y'_{n-1} \bmod p^2$ となる。ゆえに n に関する帰納法で $x_2 \equiv x'_2 \bmod p^2$ を得る。他法、E と E' で $2A$ を求めると (4.12) から

$$\begin{aligned} x'_2 - x_2 &= \left(\frac{3x_1^2 + a'_4}{2y_1}\right)^2 - 2x_1 - \left(\left(\frac{3x_1^2 + a_4}{2y_1}\right)^2 - 2x_1\right) \\ &= p\frac{6x_1^2 + 2a_4 + p}{4y_1^2} \\ &\not\equiv 0 \mod p^2 \end{aligned}$$

となり矛盾を生じる。

(ii): λ_E と $\lambda_{E'}$ が両方とも零写像であるとする。(4.11) より $\mathrm{ord}_p(x_{p-1} - x_1) \ge 2$ かつ $\mathrm{ord}_p(x'_{p-1} - x_1) \ge 2$ である。よって $x_{p-1} \equiv x'_{p-1} \bmod p^2$. すると

$$\begin{aligned} y'_{p-1} - y_{p-1} &= {x'_{p-1}}^3 - x_{p-1}^3 + a'_4 x'_{p-1} - a_4 x_{p-1} + a'_6 - a_6 \\ &\equiv x_1(a'_4 - a_4) + (a'_6 - a_6) \mod p^2 \\ &\equiv 0 \mod p^2 \end{aligned}$$

となり、(i) に矛盾する。■

系 4.8. $p \ge 7$ を素数とする。$\tilde{E}$ を $\mathbf{F}_p$ 上の anomalous epliptic curve とする。離散対数問題は時間計算量 $O((\log p)^3)$ で解ける。

証明． $\alpha, \beta \in \tilde{E}(\mathbf{F}_p) - \{\mathcal{O}\}$ とする。$\tilde{E}$ が anomalous だから $\beta = n\alpha$ となる $n \in \mathbf{F}_p$ がある。E を系 4.6 のように定める。定理 4.2 より λ_E は準同型写像だから $\lambda_E(\beta) = n\lambda_E(\alpha)$ となる。$\lambda_E(\alpha) \ne 0$ ならば $n = \dfrac{\lambda_E(\beta)}{\lambda_E(\alpha)}$ である。そうでなければ系 4.4 より λ_E は零写像である。定理 4.5(ii) と $p \ge 7$ により $u(\alpha)$, $u(2\alpha)$, $u(3\alpha)$ のうち少なくとも一つの x-座標は (4.12) を満たす。ゆえに定理 4.7 より時間計算量 $O((\log p)^2)$ で $\lambda_{E'}$ が零写像でないような E' を作ることができ、ゆえに $n = \dfrac{\lambda_{E'}(\beta)}{\lambda_{E'}(\alpha)}$ を得る。以上の時間計算量の合計は確かに $O((\log p)^3)$ である。■

上記のアルゴリズムは東京工業大学工学部電気・電子工学科：竹下望君により実際にプログラムされ実行時間が計測された。結果（各 p に対して 1 例ずつ）は以下のようになった。(CPU: Pentium-Pro, 200MHz)

p の10進での桁数	21	31	41	53
実行時間（秒）	7	17	34	61

References

1. Abel, N. H.: Aufgabe aus der Zahlentheorie. J. Reine Angew. Math. **3**, 212 (1828) (=Œuvers, 2e ed, p. 619)
2. Cassels, J. W. S.: Lectures on elliptic curves. London Mathematical Society Student Texts, 24. Cambridge: Cambridge UP 1991
3. Dickson, L. E.: History of the theory of numbers. New York: Chelsea publishing company 1966 (first print: 1919)
4. Ihara, Y.: On Fermat quotients and "the differential of numbers", Algebraic analysis and number theory, Koukyuuroku, **810**, 324-341, Kyoto: RIMS, Kyoto Univ, 1992. (in Japanese)
5. Ireland, K. and Rosen, M.: A classical introduction to mordern number theory. GTM, 84. Berlin-Heidelberg-New York: Springer 1982
6. Jacobi, C.: Beantwortung der Aufgabe Seite 212 des 3^{ten} Bandes des Crelleschen Journals: "Kann $\alpha^{\mu-1}$, wenn μ eine Primzhal und α eine Ganze Zahl und kleiner als μ und grösser als 1 ist, durch $\mu\mu$ theilbar sein?". J. Reine Angew. Math. **3**, 301-302 (1828) (=Werke vol. 6, pp. 238-239)
7. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. **48**, 203-209 (1987)
8. Lerch, M.: Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p}=q(a)$. Math. Ann. **60**, 471-490 (1905)
9. Mazur, B.: Rational points of Abelian varieties with values in towers of number fields. Invent. Math. **18**, 183-266 (1972)
10. McCurley, K. S.: The discrete logarithm problem, Proc. Sympos. Applied Math., **42**, 49-74, 1990.
11. Menezes, A. J., Okamoto, T. and Vanstone, S. A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Info. Theory **39**, 1639-1646 (1993)
12. Miller, V. S.: Use of elliptic curves in cryptography, Advances in cryptology-CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., **218**, 417-426, Berlin-Heidelberg-New York: Springer, 1986.
13. Pohlig, S. C. and Hellman, M. E.: An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. IEEE Trans. Info. Theory **24**, 106-110 (1978)
14. Ribenboim, P.: The new book of prime number records, 3rd ed. Berlin-Heidelberg-New York: Springer 1995
15. Rüeck, H. G.: On the Discrete Logarithm in the Divisor Class Group of Curves, (1997). preprint
16. Semaev, I. A.: Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p. Math. Comp. **67**, 353-356 (1998)
17. Serre, J.-P.: A course in arithmetic. GTM, 7. Berlin-Heidelberg-New York: Springer 1973
18. Silverman, J. H.: The arithmetic of elliptic curves. GTM, 106. Berlin-Heidelberg-New York: Springer 1985
19. Smart, N. P.: The discrete logarithm problem on elliptic curves of trace one, (1997). preprint
20. Voloch, J. F.: Relating the Smart-Satoh-Araki and Semaev approaches to the discrete logarithm problem on anomalous elliptic curves, (1997). preprint, Available at http://www.ma.utexas.edu/users/voloch